

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ  
ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

**ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ**

**Кафедра інформаційної безпеки**

**КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2**

з дисципліни

Криптографія

З теми: «Криптоаналіз шифру Віженера»

Перевірила:

Селюх П.В

Виконали студенти групи ФБ-94

Спільна А.С. та Артюшенко В.В.

**Мета роботи:**

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

### Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини  $r = 2, 3, 4, 5$ , а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Код програми знаходиться в Crypto2.cpp ;

Результати в файлі Crypto2\_results.xlsx ;

Зашифрований текст Варіанта 6 в файлі variant6.txt;

Розшифрований текст в файлі deciphervar6.txt;

### Результати:

Текст	Індекс
ВТ	0,0543972
$r = 2$	0,0458914
$r = 3$	0.0397793
$r = 4$	0,038509
$r = 5$	0,0360037
$r = 12$	0,0354397

Для розшифрування спочатку потрібно було визначити яку довжину має ключ, нашого шифрованого тексту за варіантом.

Для цього ми шукали індекси відповідності кожного блоку для ймовірної довжини ключа, і на той яка нам підходить ми бачимо явну різку зміну в значеннях, знизу декілька прикладів:

```
Введите предполагаемый ключ :
2
Количество символов в файле : 6853
0.034185
0.0339538
Для продолжения нажмите любую клавишу . . .

Введите предполагаемый ключ :
7
Количество символов в файле : 6853
0.0343262
0.0339105
0.0340567
0.0342238
0.0341403
0.0350761
0.0337204
Для продолжения нажмите любую клавишу . . .
```

```
>> : 14
Введите предполагаемый ключ :
14
Количество символов в файле : 6853
0.0338764
0.0333819
0.034153
0.0342452
0.0342703
0.0352342
0.0335496
0.0341279
0.0340273
0.0337759
0.0345302
0.0342033
0.0348486
0.0341865
Для продолжения нажмите любую клавишу . . .
```

```
>> : 17
Введите предполагаемый ключ :
17
Количество символов в файле : 6853
0.0576152
0.0596768
0.0522944
0.052924
0.0621458
0.0549609
0.0529733
0.0547881
0.0532326
0.0563189
0.051961
0.058504
0.0569115
0.0534672
0.0570473
0.0555782
0.0558498
Для продолжения нажмите любую клавишу . . .
```

Можна замітити, що на 17 значно підвищилось значення індексу відповідності, отже можна вважати, що наш ключ, має довжину в 17 символів.

Далі потрібно, було знайти сам ключ, для цього з кожного блоку, знаходимо літери, які частіше зустрічаються, в нашому варіанті це:

```
>> : 7
Количество символов в файле : 6853
рхрюзууцтфццо
```

Я їх записала в масив.

Тепер, залишилось тільки за допомогою шифру цезаря, знайти слово-ключ, для цього берем найчастішу букву з наших блоків і віднімаємо її індекс від індексу найчастішої літери в російській мові («о») по модулю 32 і знаходимо сам ключ:

```
Количество символов в файле : 6853
рхрюзууцтфцто
Введите самую частую букву русского алфавита : о
возвращениеджинда
Для продолжения нажмите любую клавишу . . . █
```

Получаємо словосполучення : возвращениеджинда

Тепер спробуємо розшифрувати текст:

```
>> : 8
Введите ключ : возвращениеджинда

Размер ключа : 17
Для продолжения нажмите любую клавишу . . . █
```

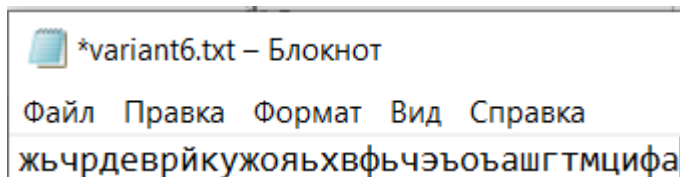
Отримуємо майже правильно розшифрований текст:

дорофейльвовичпсвторыкобылыниразъвжизнинепокидалзomлхотяпрожилужекошьшес

Аналізуємо:

33 літера «ъ», явно повинна бути «у», тому що ниразУвжизни:

Тому за допомогою знань про шифр Віжинера, ми знаходимо правильну 16 літеру для нашого ключа:



33 буква в зашифрованому тексті це А, яка має індекс 0, а У індекс 19, щоб отримати У, нам потрібно:

$$0 - ? \bmod 32 = 19$$

Це число буде 13, а літера з таким індексом, то Н,

Отже, в знайденому ключі потрібно 16 літеру замінити на Н, тоді ми отримуємо словосполучення-ключ: **возвращениеджинна**

І справді при розшифруванні все проходить чудово!!!

Ось розшифрований текст:

дорофейльвовичпивторыкобылыниразувжизнинепокидалземлихотяпрожилужебольшешестидесятилетработалпрорабомстроительнойкомпаниидомостройвхарьковестолицевкраинылюбилпорыбачитьсдрузьяминаозерахроганьскогокраязачертойгородавыращивалнадачномучасткеовощиифруктывоспитывалвнуковавотуезжатьзапределыроднойвкраинынелюбилнесмотрянавозможностивсвязиссозданиемглобальнойсетиметропобыватьналюбойпланетесолнечнойсистемыидажезаеепределамичтоподвиглоегосогласитьсянаэкскурсиюполунеонисамневсостояниибылоответитьвероятносыгралисвоюрольрассказыдрузейхваставшихсясвоимипутешествиямиунеговыигралоллюбопытствопосмотретьвблизичтожеэтотакоеспутницаземлиокоторойтакмногоговорятдетивнукиидрузьякакбытонибылоаутромдвадцатьтретьегодекабрякакратвначалосвятокдорофейльвовичвтайнеотродныхиблизкихпозвонилвбюроэкскурсийсолнечнойсистемызапнаясьобъяснилчегохочетивтотжеденьпомощьюметродобралсядоаполлонтаунагороданалунеоткудадолжнабыланачатьсяэкскурсияпосамымкрасивымизагадочнымместамспутницыземлиаполлонтаунарасполагалсянаравнинеморяспокойствиянедалекоотзнаменитойбороздымаскелайнапохожейнаизвилистоеруслорекиименноздеськогдавконцедвадцатоговекасовершилпосадкуамериканскийпилотируемыйкорабльаполлонодиннадцаточнееегопосадочныймодульестественноэкскурсантамзанимавшимкабинудвадцатиместногоэкскурсионногофлайтасначалапоказалипамятникаполлонуодинадцатьпирамидуизлунногобазальтаспосадочнойплатформойиамериканскимфлагомазатемфлайтотправилсявпутешествиепоморяспокойствиязалитомуяркимсолнечнымсветомэкскурсантамиоказалисьмолодыелюдиввозрастеотвосемнадцати до двадцати лет поэтому поначалу дорофейльвович чувствовал себя не в своей тарелке смущаясь под любопытными взглядами спутников но потом его захватила суровая красота лунных пейзажей и он перестало обращать внимания на веселящуюся компанию жадно разглядывая проплывающие под днищем флайта цирки эскарпы кратеры живописные группы скал мореспокойствия получили свое название не случайно его ровная гладкая поверхность типична для обширных морей на дневной стороне луны и редкорядует наблюдателей проявлением вулканической деятельности однако из здесь имело сьемало интересных мест объектов которые десятилетиями волновали астрономов изучающих спутницу земли загадочная цепочка кратеров под названием теннисная ракетка около двух десятков в диаметре от пятидесяти до ста метров протянулись удивительно ровной линией заканчиваясь кратером побольше диаметра около шестисот метров впечатление складывается такое будто по лунной поверхности действительно прокатился подпрыгивая теннисный мяч оставив в пыли цепочку следов совиный мост каменная арка через борозду маскелайна длиной около трех километров изумительно ровная стена обрывается длиной около тридцати километров будто кто-то отхватил ножом кусок лунной поверхности и выбросил в космос оставив срезы ложбин углубиной в километр борозда золотой ручей сама настоящая русла реки шириной в полтора километра и глубиной в полтора метра сверкающее под лучами солнца кристалликами пирита цветочная клумба возвышения рыхлой породы оранжевого цвета диаметром около двух километров ввысотой в двести метров действительно клумба если посмотреть сверху стоунхендж группы скал плоскими вершинами соединенных поверху доточноровными плитами практически не отличается от земного мегалитического комплекса англия и наконец борозда маскелайна длиной около четырех сот километров также здорово похожая на русла реки шириной от километра до трех как бы сгладил борозда сама по себе представляет собой сдвиговой разлом лунной коры случившийся десятилетиями назад в результате подвижки штаута удар метеорита на поверхность борозда все равно напоминает реку и дорофейльвович даже представил как по руслу течет вода она навливались и выходили из флайта одеты в пузыри вакуума плотных спецов в несколько коразв кабине аппарата под давлением нормальной силы тяжести почти земная а вне ее царил лунный нетяготение в шесть раз слабее земного поэтому не обошлось без курьезов и неловких движений правда все в конце концов привыкли к необычайной легкости в теле и удовольствию скакали по местным буеракам в том числе и дорофейльвович получивший не с чем не сравнимые ощущения теперь я вам покажу объект зоро сказал гид приглашая экскурсанта в кабину после очередного выхода на наружу ходят легенды что в этом месте на глубине двух сот метров располагался загадочный шар из которого впоследствии вылутился на земную боевой гипертеридский робот демон авторитетным тоном заметил кто то из компании молодых людей или джинн совершенно верно новедь он потом оставил в кольцах сатурна свою юбку рубиллиантиды это уже другая история вы наверняка помните вой на джинна из закончилась всего лишь год назад здесь остался след демона чтовне интересно увидете флайт прозрачными до самого пола стенками поднялся над кратером а вакава и понесся к горизонту свисаящей над ним почти

полной землей окрашивающей равнину в голубоватый цвет в местах где лежал атень от скал освещенных прямыми солнечными лучами приблизилась река борозды маскелайн раздалась вширь превратилась в крутой глубиной до километра каньон на одном из плоских гребней каньона появилось белосеребристое пятнышко превратилось в холмик затем в горус дырой в центре флайт завис в паре километров от этой странной горы и экскурсенты начали рассматривать объект и веший необычно название эзеро больше всего серебристый купол кратером диаметром в три километра на поминал человеческий глаз радужка которого высохла и пожухла превратившись в белоснежный слой мха и вызвал этот глазотнюдь неприятные и радостные ощущения не омерзение нет но не восторг слишком много в этом зрелище было пугающего и отталкивающего и одновременно притягивающего в зорь молодёжь притихла дорфейльвович почувствовал стеснение в груди посмотрел на гидатотулыбнул ся как настоящий человек хотя был всего на всего витсом нравиться что это такое эффект квантовой эффузии как говорят ученые образно говоря на горные породы действовало дыхание демона на этом месте более двух сот лет назад находился ториевый рудник шахта которого достигла шаровидной полости где и спал джинн непосредственно к шахте нас не пропустили охрана тут рядом есть интересное ущелье оно образовалось совсем недавно всего два месяца назад мы можем полюбоваться на рудник со брыва полетели из дорво очень интересномых хотим прогуляться раздались голоса дорфейльвович хотя и не испытывал большого желания гулять однако возражать не стал у него возникло ощущение что он здесь уже был когда то хотя и некого дараньшелуну не посещал флайтоблетел снежно серебристый глаз бывшего ториевого рудника кругом повернувшись вдоль борозды маскелайн к югу снизился стали видны трещины разорвавшие боковые стены борозды все свежее судя по блеску узкие и пошире очевидно это был результат недавнего лунотрясения о котором говорил гид приблизилась очередная трещина действительно образовавшая живописное ущелье с слоистыми стенами флайт подпрыгнул исел на обрыве которого были хороши видны куполообразные борозды маскелайн экскурсенты посыпались из аппарата радуясь возможности размяться гурьбой направились к брыву перебрасываясь шуточками и дурачась в них игра лащения чья энергия молодости и дорфейльвовичам гновение не позабывал задор и оптимизм у юношей и девушек годящихся ему чуть ли не в внуки он тоже полюбовался на снежно белый купол в трех километрах от брыва потом тихонько отошел от резвящихся молодых людей и пошелся вдоль обрыва вглядываясь в противоположную стену ущелья вглядываясь в ряд черных отверстий похожих на следы пулеметной очереди и заинтересовался дорфейльвович прыгнул вниз и в ключив антиграв пересек ущелье опустился на узкий карниз перед самой большой дырой на предупреждении гида не отходить далеко от флайта он забыл дыра оказалась входом в пещеру

**Висновок:** Виконавши дану практичну роботу, засвоїла навички з шифрування та розшифрування тексту з відомим ключем. А також власноруч розшифрувати тест незнаючи ключа, за допомогою пошуку довжини ключа індексами відповідності, та шифром Цезаря, використовуючи найчастіше зустрічаємі літери.